(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
23 décembre 2004 (23.12.2004)

PCT

(10) Numéro de publication internationale
WO 2004/111833 A1

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/EP2004/051142

(22) Date de dépôt international : 17 juin 2004 (17.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0307380 18 juin 2003 (18.06.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : GEMPLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, F-13420 Gemenos (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : JOYE, Marc [BE/FR]; Traverse des Jardins, F-83640 Saint Zacharie (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR COUNTERMEASURING IN AN ELECTRONIC COMPONENT

(54) Titre : PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE

(57) Abstract: The invention relates to a method for countermeasuring in an electronic component while using a public key cryptographic algorithm. The invention involves the use of a public key cryptographic algorithm containing an exponentiation calculation y=g^d, in which g and y are elements of specified group G noted in a multiplicative manner and d is a predetermined number.

(57) Abrégé : La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de chiffrement à clé publique. Le procédé de la présente invention met en oeuvre un. algorithme cryptographique à clé publique, comprenant un calcul d'exponentiation de type y=g^d où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé.

WO 2004/111833 A1